

# METHOD, DEVICE AND PROGRAM FOR ISSUING CERTIFICATE, MEDIUM WHERE THE PROGRAM IS RECORDED, METHOD, DEVICE AND PROGRAM FOR ISSUING CERTIFICATE, AND MEDIUM WHERE THE PROGRAM IS RECORDED

Publication number: JP2002374401

Publication date: 2002-12-26

Inventor: SAKAGAMI KOICHI; KAMISAKA TAKESHI

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- International: G06Q50/00; G06T1/00; H04N1/387; G06Q50/00;  
G06T1/00; H04N1/387; (IPC1-7): H04N1/387;  
G06F17/60; G06T1/00

- European:

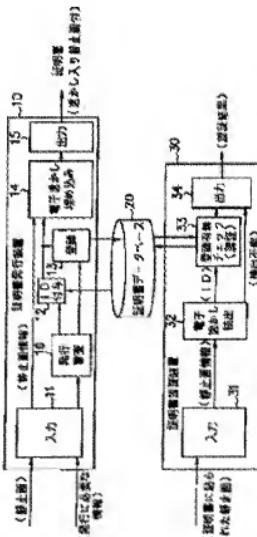
Application number: JP20010182211 20010615

Priority number(s): JP20010182211 20010615

[Report a data error here](#)

## Abstract of JP2002374401

**PROBLEM TO BE SOLVED:** To actualize the issue of a certificate and authentication in which a person can not illegally obtain the certificate and impersonate the very person even in the case of changing the photograph attached. **SOLUTION:** Personal information on a user is inputted from an input means 11 and a still picture is processed into electronic information; and an ID is imparted by an ID imparting means 12 and the ID and personal information are registered in a certificate DB20 while making it correspond to each other, and an electronic watermark embedding means 14 embeds the ID as an electronic watermark in the still picture information to issue a certificate including it. The still picture included in the certificate is inputted as electronic information from an input means 31, an electronic watermark detecting means 32 detects the ID embedded as the electronic watermark to judge whether the detected ID is registered in the certificate database 20, thereby outputting an authentication result showing that the certificate is genuine when the ID is registered or false when the ID is not detected or registered.



Data supplied from the [esp@cenet](mailto:esp@cenet) database - Worldwide

**Family list**

1 family member for: **JP2002374401**

Derived from 1 application

[Back to JP2002374](#)

- 1 METHOD, DEVICE AND PROGRAM FOR ISSUING CERTIFICATE,  
MEDIUM WHERE THE PROGRAM IS RECORDED, METHOD, DEVICE  
AND PROGRAM FOR ISSUING CERTIFICATE, AND MEDIUM WHERE  
THE PROGRAM IS RECORDED**

Inventor: SAKAGAMI KOICHI; KAMISAKA TAKESHI Applicant: NIPPON TELEGRAPH & TELEPHONE

EC:

IPC: G06Q50/00; G06T1/00; H04N1/387 (+6)

Publication info: **JP2002374401 A** - 2002-12-26

---

Data supplied from the **esp@cenet** database - Worldwide

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-374401

(P2002-374401A)

(43)公開日 平成14年12月26日 (2002.12.26)

| (51)Int.Cl. <sup>7</sup> | 識別記号  | F I          | マーク <sup>8</sup> (参考) |
|--------------------------|-------|--------------|-----------------------|
| H 04 N 1/387             |       | H 04 N 1/387 | 5 B 0 5 7             |
| G 06 F 17/60             | 1 4 0 | C 06 F 17/60 | 1 4 0                 |
| G 06 T 1/00              | 5 0 0 | C 06 T 1/00  | 5 0 0 B               |

審査請求 未請求 請求項の数 8 O.L (全 8 頁)

(21)出願番号 特願2001-182211(P2001-182211)

(22)出願日 平成13年6月15日 (2001.6.15)

(71)出願人 000004226  
日本電信電話株式会社  
東京都千代田区大手町二丁目3番1号

(72)発明者 阪上 異一  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内

(73)発明者 上坂 剛  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内

(74)代理人 100069981  
弁理士 吉田 精季

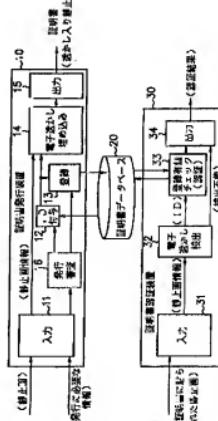
最終頁に続く

(54)【発明の名稱】 証明書発行方法、その装置、そのプログラム及びそのプログラムを記録した媒体、並びに証明書認証方法、その装置、そのプログラム及びそのプログラムを記録した媒体

(57)【要約】

【課題】 証明書を不正に入力し、写真を張り替えても本人に成りすますことが不可能な証明書の発行及び認証を実現すること。

【解決手段】 入力手段11から利用者の個人情報を入力とともに静止画を電子情報化して入力し、ID付与手段12にてIDを付与し、IDと個人情報を対応づけて証明書DB20に登録し、電子透かし埋め込み手段14によりIDを静止画情報に電子透かしとして埋め込み、これを含む証明書を発行するとともに、入力手段31から証明書に含まれる静止画を電子情報化して入力し、電子透かし検出手段32により静止画情報から電子透かしによるIDを検出し、検出したIDが証明書データベース20に登録されているかを判断し、登録されていれば正当とし、IDが検出されないまたは登録されていなければ不正とする認証結果を出力する。



## 【特許請求の範囲】

【請求項1】 利用者本人かどうかを証明するための証明書を発行する証明書発行方法であって、証明書発行に必要な利用者の個人情報を入力するとともに利用者本人の静止画を電子情報化して入力し、

利用者毎に固有の識別情報を付与し、

前記識別情報と前記個人情報を対応づけて証明書データベースに登録し、

前記識別情報を電子透かしとして前記静止画情報に埋め込み、

前記電子透かしが埋め込まれた静止画を含む証明書を出力することを特徴とする証明書発行方法。

【請求項2】 利用者本人かどうかを証明するための証明書を発行する証明書発行方法であって、証明書発行に必要な利用者の個人情報を入力するとともに利用者本人の静止画を電子情報化して入力する手段と、

利用者毎に固有の識別情報を付与する手段と、

前記識別情報と前記個人情報を対応づけて証明書データベースに登録する手段と、

前記識別情報を電子透かしとして前記静止画情報に埋め込む手段と、

前記電子透かしが埋め込まれた静止画を含む証明書を出力する手段とを備えたことを特徴とする証明書発行装置。

【請求項3】 利用者本人かどうかを証明するための証明書を発行する証明書発行プログラムであって、

該プログラムはコンピュータに、

証明書発行に必要な利用者の個人情報を入力するとともに利用者本人の静止画を電子情報化して入力し、

利用者毎に固有の識別情報を付与し、

前記識別情報と前記個人情報を対応づけて証明書データベースに登録し、

前記識別情報を電子透かしとして前記静止画情報に埋め込み、

前記電子透かしが埋め込まれた静止画を含む証明書を出力する動作を実行させることを特徴とする証明書発行プログラム。

【請求項4】 請求項3記載の証明書発行プログラムを記録したことを特徴とする証明書発行プログラムを記録した媒体。

【請求項5】 利用者毎に付与された識別情報が電子透かしとして埋め込まれた利用者本人の静止画を含む証明書の正当性を、利用者毎の固有の識別情報と証明書発行に必要な利用者の個人情報を対応づけて登録した証明書データベースを用いて認証する証明書認証方法であつて、

証明書に含まれる静止画を電子情報化して入力し、

前記静止画情報から電子透かしによる識別情報を検出し、

前記検出した識別情報が証明書データベースに登録されているかを判断し、

登録されていれば正当とし、識別情報が検出されないまたは登録されていなければ不正とする認証結果を出力することを特徴とする証明書認証方法。

【請求項6】 利用者毎に付与された識別情報が電子透かしとして埋め込まれた利用者本人の静止画を含む証明書の正当性を、利用者毎の固有の識別情報と証明書発行に必要な利用者の個人情報を対応づけて登録した証明書データベースを用いて認証する証明書認証装置であつて、

証明書に含まれる静止画を電子情報化して入力する手段と、

前記静止画情報から電子透かしによる識別情報を検出する手段と、

前記検出した識別情報が証明書データベースに登録されているかを判断する手段と、

登録されていれば正当とし、識別情報が検出されないまたは登録されていなければ不正とする認証結果を出力する手段とを備えたことを特徴とする証明書認証装置。

【請求項7】 利用者毎に付与された識別情報が電子透かしとして埋め込まれた利用者本人の静止画を含む証明書の正当性を、利用者毎の固有の識別情報と証明書発行に必要な利用者の個人情報を対応づけて登録した証明書データベースを用いて認証する証明書認証プログラムであつて、

該プログラムはコンピュータに、

証明書に含まれる静止画を電子情報化して入力し、前記静止画情報から電子透かしによる識別情報を検出し、

前記検出した識別情報が証明書データベースに登録されているかを判断し、

登録されていれば正当とし、識別情報が検出されないまたは登録されていなければ不正とする認証結果を出力する動作を実行させることを特徴とする証明書認証プログラム。

【請求項8】 請求項7記載の証明書認証プログラムを記録したことを特徴とする証明書認証プログラムを記録した媒体。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、個人向けの証明書を発行する方法、その装置、そのプログラム及びそのプログラムを記録した媒体、並びに該証明書を認証する方法、その装置、そのプログラム及びそのプログラムを記録した媒体に関する。

## 【0002】

【従来の技術】 従来、例えば、身分証明書で本人を確認する場合、(1)身分証明書内の識別番号、(2)身分証明書に表示された写真、(3)パスワード、等を手が

かりに本人かどうかの確認・認証を行っていた。

### 【0003】

【発明が解決しようとする課題】しかし、この方法では、身分証明書やパスワードが盗まれ、写真が貼り替えられた場合、本人に成りますことが可能であるという問題があった。

【0004】本発明の目的は、従来の身分証明書で発生する成りますしの問題を解決し、証明書を不正に入手し、写真を張り替えても本人に成りますことが不可能な証明書の発行及び認証を実現することにある。

### 【0005】

【課題を解決するための手段】前記課題を解決するため、本発明では、利用者本人かどうかを証明するための証明書を発行する証明書発行方法であって、証明書発行に必要な利用者の個人情報を入力するとともに利用者本人の静止画を電子情報化して入力し、利用者毎に固有の識別情報を付与し、前記識別情報と前記個人情報を対応づけて証明書データベースに登録し、前記識別情報を電子透かしとして前記静止画情報に埋め込み、前記電子透かしが埋め込まれた静止画を含む証明書を出力する証明書発行方法を提案する。

【0006】また、利用者毎に付与された識別情報が電子透かしとして埋め込まれた利用者本人の静止画を含む証明書の正当性を、利用者毎の固有の識別情報と証明書発行に必要な利用者の個人情報を対応付けて登録した証明書データベースを用いて認証する証明書認証方法であって、証明書に含まれる静止画を電子情報化して入力し、前記静止画情報から電子透かしによる識別情報を検出し、前記検出した識別情報が証明書データベースに登録されているかを判断し、登録されていれば正当とし、識別情報が検出されないまたは登録されていなければ不正とする認証結果を出力する証明書認証方法を提案する。

【0007】前記証明書発行・認証方法によれば、例えば証明書を不正に入手した者が証明書の写真を自分の写真貼り替えて、その写真から電子透かしによる識別情報が検出されないため、証明書の正当性が認証されず、本人に成りますことは不可能となる。

【0008】なお、ここで、使用的する電子透かしの埋め込み・検出方式（アルゴリズム）は非公開とし、当事者以外は電子透かしから識別情報を読み取ることも、電子透かしとして識別情報を埋め込むこともできない方式とする。

【0009】なお、電子透かし技術については、例えば「日経エレクトロニクス、No. 683、1997. 2. 24. p. 116-147」に記載されているものその他、種々の方式が知られているので、本明細書では、「電子透かし埋め込み装置（手段）」及び「電子透かし検出装置（手段）」についての詳しい説明を省略する。

### 【0010】

【発明の実施の形態】本発明の実施の形態について、図面を参照しながら説明する。

【0011】図1は、本発明の実施の形態の一例を示すもので、図中、10は証明書発行装置、20は証明書データベース、30は証明書認証装置である。

【0012】証明書発行装置10は、証明書発行に必要な利用者の個人情報（氏名、住所、連絡先電話番号等）を入力するとともに利用者本人の静止画（写真等）を電子情報化して入力する入力手段11と、利用者毎に固有（既に付与済みでない唯一無二の）の識別情報（ID）（通常、複数ビットのディジタルデータ）を付与するID付与手段12と、前記IDと前記個人情報を対応づけて証明書データベース20に登録する登録手段13と、前記IDを電子透かしとして前記静止画情報に埋め込む電子透かし埋め込み手段14と、前記電子透かしが埋め込まれた静止画（人が見ただけでは電子透かしが埋め込まれていることは感知できない。）を含む証明書を出力（印刷）する出力手段15とからなっている。

【0013】なお、証明書発行に必要な利用者の個人情報を基に証明書発行の適否を審査する発行審査手段16を設けて、審査に合格した場合のみIDを付与し、証明書を発行するようにならう。

【0014】証明書データベース20は、図2に示すように、利用者毎の固有のIDと証明書発行に必要な利用者の個人情報とが対応付けて登録されている。

【0015】証明書認証装置30は、証明書に含まれる静止画を電子情報化して入力する入力手段31と、前記静止画情報から電子透かしによるIDを検出する電子透かし検出手段32と、前記検出したIDが証明書データベース20に登録されているかを判断する登録有無チェック（認証）手段33と、登録されていれば正当とし、IDが検出されないまたは登録されていなければ不正とする認証結果を出力する出力手段34とからなっている。

【0016】図3は、図1の証明書発行装置における処理のフローチャート、図4は、図1の証明書認証装置における処理のフローチャートである。

【0017】まず、図3に従い、証明書発行処理について述べる。

【0018】（ステップ1）証明書発行に必要な利用者の個人情報を入力するとともに利用者本人の静止画を電子情報化して入力する（41）。

【0019】（ステップ2）利用者毎に固有のIDを付与する（42）。

【0020】（ステップ3）前記IDと前記個人情報を対応づけて証明書データベースに登録する（43）。

【0021】（ステップ4）前記IDを前記静止画情報に電子透かしとして埋め込む（44）。

【0022】（ステップ5）前記電子透かしが埋め込ま

れた静止画を含む証明書を出力する(45)。

【0023】なお、必要に応じて証明書発行に必要な利用者の個人情報を基に証明書発行の適否を審査するステップを設けて、審査に合格した場合のみIDを付与し、証明書を発行するようになても良い(46)。

【0024】次に、図4に従い、証明書認証処理について述べる。

【0025】(ステップ1) 証明書に含まれる静止画を電子情報化して入力する(51)。

【0026】(ステップ2) 前記静止画情報から電子透かしによるIDを検出する(52)。

【0027】(ステップ3) IDが検出された場合、該検出されたIDが証明書データベースに登録されているかをチェックする(53)。

【0028】(ステップ4) 検出されたIDが証明書データベースに登録されていれば正当とし、IDが検出されなかった場合または証明書データベースに登録されていない場合は不正とする認証結果を出力する(54)。

【0029】図5は、本発明の証明書発行装置及び証明書認証装置に対し、ネットワークを介して証明書の発行または認証を依頼するシステム全体の構成を示すもので、図中、6.1は図1に示した証明書発行装置、証明書データベース及び証明書認証装置からなる証明書発行認証装置群、6.2は証明書の発行を依頼する証明書発行依頼端末、6.3は証明書の認証を依頼する証明書認証依頼端末、6.4はこれらを接続するネットワークである。

【0030】図6は、前記証明書発行依頼端末または証明書認証依頼端末の具体例を示すものである。

【0031】同図(a)は利用者本人の静止画または証明書に含まれる静止画がデジタルカメラ等により電子情報化されている場合に適した例を示しており、モデル等を含むパーソナルコンピュータ(PC)を用いて証明書発行依頼端末または証明書認証依頼端末を実現している。この例の場合、前記静止画情報はネットワークを介して証明書発行認証装置群の入力手段を実現するPCサーバに入力される。なお、証明書はPCに接続されたプリンタにより印刷出力することができ、認識結果は画面上に表示出力あるいはプリンタより印刷出力ができる。

【0032】同図(b)は利用者本人の静止画または証明書に含まれる静止画が電子情報化されていない場合に適した例を示しており、ファクシミリを用いて証明書発行依頼端末または証明書認証依頼端末を実現している。この例の場合、前記静止画はファクシミリで読み取られて電子情報化され、ネットワークを介して証明書発行認証装置群の入力手段を実現するFAXサーバに入力される。なお、証明書、認識結果とも、ファクシミリにより印刷出力ができる。

【0033】なお、同図(b)の例において証明書発行依頼端末を実現した場合の証明書発行に必要な利用者の

個人情報の入力については、予め用意した所定の様式を有する依頼書に個人情報を書き込ませ、この依頼書を静止画と同様にファクシミリで読み取らせてその画像データをFAXサーバ間に送り、サーバ側で該画像データ中から文字認識技術を利用して個人情報を取り出すようにすれば良い。

【0034】図7は、本発明を利用した証明書発行・認証サービスの具体例、ここでは本発明の証明書発行認証装置群を運営する証明書発行・認証事業者の提携組織グループに属する会員制クラブに適用した例の概要を示す。本例は、

- ・会員制クラブの運営者が会員としての身分証明書を発行する(場面1)、

- ・クラブを利用したい会員が身分証明書を提示し、会員制クラブの運営者がそれを認証することで会員であるとの確認を行う(場面2)、

より構成する。

【0035】図8は本例における会員登録(証明書発行)の際の流れ、図9は本人確認(証明書認証)の際の流れを示すものである。

【0036】まず、図8に沿って、会員登録の場合の処理について述べる。

【0037】《ステップ1：会員登録依頼》会員登録希望者は、会員登録に必要な個人情報(例えは、氏名、住所、連絡先の電話番号等)、会員証を使用する本人の写真などを入力する(71)。入力されたデータは、会員制クラブの運営者もしくはその代理店(=登録受け付け者)に伝えられる(72)。伝える方法としては、直接の手渡し、郵送の他、ファクシミリ、写真データ添付によるインターネットメール送付等のネットワークを介して行う、等の方法がある。

【0038】《ステップ2：証明書発行依頼》登録受け付け者は、ステップ1で伝えられた情報を証明書発行依頼端末より入力する(73)。証明書発行依頼端末から入力されたデータは、本発明の証明書発行認証装置群に入力される(74)。

【0039】《ステップ3：証明書発行処理》証明書発行認証装置群は、会員IDを付与し、会員DB(証明書DB)に登録するとともに電子透かしを入れた写真を生成し(75)、証明書として出力する(76)。

【0040】《ステップ4：会員証発行》登録受け付け者は、電子透かし入りの写真を貼った会員証を発行する(77)。

【0041】《ステップ5：会員証配送》会員証を新規会員に渡す(78)。会員証の送付には、郵送、ファクシミリ、メール添付等の方法がある(いずれの場合も、写真に埋め込んだ電子透かしは保存される)。

【0042】次に、図9に沿って、会員認証の場合の処理について述べる。

【0043】《ステップ1：会員証提示》会員は、会員

制クラブ利用の際、会員制クラブの運営者もしくはその代理店、加盟店組織（店舗など）（=認証者）に、身分証明書を提示する（81、82）。直接提示の他、ファクシミリ、インターネットメールに添付することで、ネットワークを介して身分証明書のイメージ写真を送る行う方法がある。

【0044】**【ステップ2：証明書認証依頼】**認証者は、ステップ1で提示されたデータ（身分証明書写真等）を証明書認証依頼端末に入力する（83）。証明書認証依頼端末から入力されたデータは、本発明の証明書発行認証装置群に入力される（84）。

【0045】**【ステップ3：証明書認証処理】**証明書発行認証装置群は、身分証明書の正当性を審査し（85）、認証結果を通知する（86）。正当性の審査の詳細については図1、図4の説明を参照のこと。

【0046】**【ステップ4：本人確認】**認証者は、前記審査の結果（身分証明書の正当性）と、身分証明書の写真と本人の顔との合致を確認し、本人性を判断する（87）。写真と本人の顔との合致は、会員と認証者とが離れている場合、ネットワークを介してテレビ電話、ディジタルカメラ伝送、等を用いる方法もある。

【0047】図1は、本発明を利用した証明書発行・認証サービスの事業形態を示すものである。

【0048】利用者に証明書発行・認証サービスを提供しようとする事業者、ここではその傘下にクラブ加盟事業者（チェーン店等）を抱える会員制クラブ運営事業者（チェーン店経営事業者等）は、事前に証明書発行認証装置群を運営する証明書発行・認証事業者との間で証明書発行・認証サービスの契約を結んでおり、クラブ加盟事業者から徴収するフランチャイズライセンス料の中から契約料を証明書発行・認証事業者に支払う。

【0049】証明書発行・認証事業者は各クラブ加盟事業者に証明書発行依頼端末及び証明書認証依頼端末を設置し、該端末からのアクセスに応じて証明書発行認証装置群により証明書の発行・認証を行う。

【0050】なお、バリエーションとして、本発明の構成要素のうち、証明書発行装置、証明書データベース、証明書認証装置をそれぞれネットワーク上の別のサイトで実現する形態や別の事業主体とする運営も考えられ

る。また、証明書発行装置に発行審査手段を設ける場合、さらにこれを別のサイトで実現する形態や別の事業主体とする運営も考えられる。

【0051】なお、本発明は、CPU、メモリ、外部記憶装置等からなる周知のコンピュータに媒体もしくは通信回線を介して、図1の構成図に示された機能を実現するソフトウェア（プログラム）あるいは図3、図4のフローチャートに示された手順を備えるソフトウェア（プログラム）をインストールすることによっても実現可能である。

【0052】

**【発明の効果】**以上説明したように、本発明によれば、写真の張り替えによる本人なりすましを防ぐことができ、低コストで確実な身分証明書の発行・認証を行うことが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態の一例を示す構成図

【図2】証明書データベースの一例を示す説明図

【図3】証明書発行装置における処理のフローチャート

【図4】証明書認証装置における処理のフローチャート

【図5】本発明装置にネットワークを介して証明書の発行または認証を依頼するシステム全体を示す構成図

【図6】証明書発行依頼端末または証明書認証依頼端末の具体例を示す説明図

【図7】本発明を利用して証明書発行・認証サービスの具体例を示す説明図

【図8】図7の例における会員登録（証明書発行）の際の流れ図

【図9】図7の例における本人確認（証明書認証）の際の流れ図

【図10】本発明を利用して証明書発行・認証サービスの事業形態を示す説明図

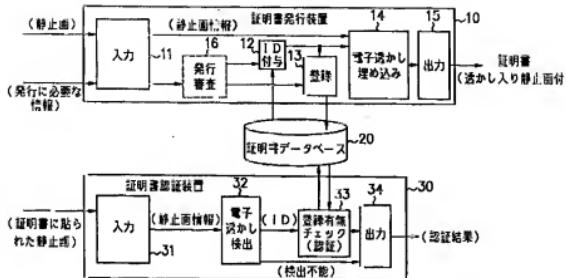
【符号の説明】

10：証明書発行装置、11：入力手段、12：ID付与手段、13：登録手段、14：電子透かし埋め込み手段、15：出力手段、20：証明書データベース、30：証明書認証装置、31：入力手段、32：電子透かし検出手段、33：登録有無チェック（認証）手段、34：出力手段。

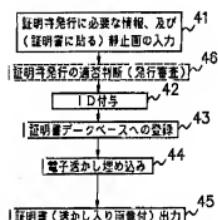
【図2】

| JD   | 個人情報                      |
|------|---------------------------|
| XXXX | ☆山〇夫、◎◎市△△町1-1-1、***-88#8 |
| YYYY | 口田△子、▽▽市△△町2-2-2、@@@-5555 |
|      |                           |

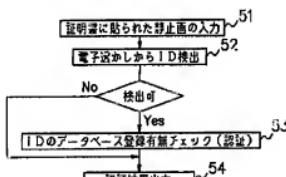
【図1】



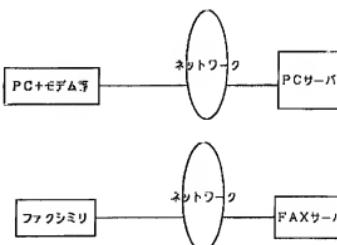
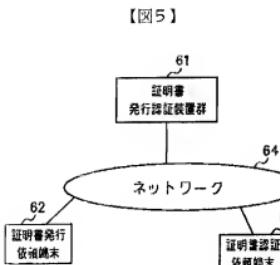
【図3】



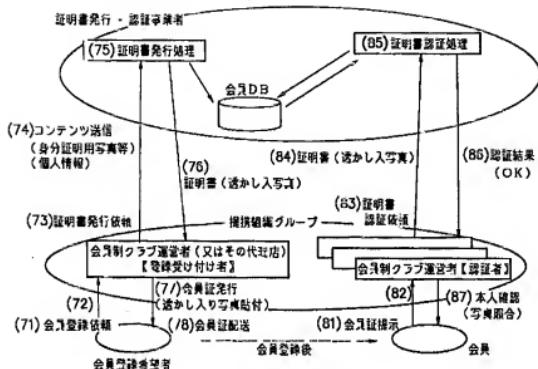
【図4】



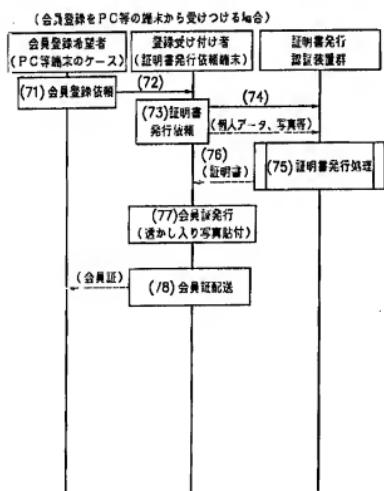
【図6】



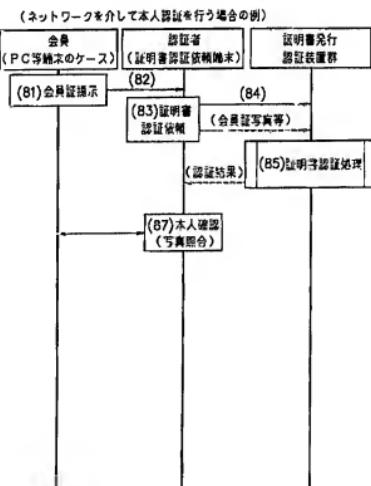
【図7】



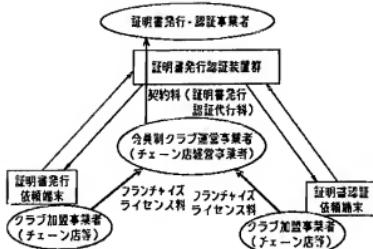
【図8】



【図9】



【図10】



フロントページの続き

Fターム(参考) 5B057 CA08 CA12 CA16 CB08 CB12  
CB16 CB08 CG07  
5C076 AA14 BA06